REMARKS

I. INTRODUCTION

In response to the Office Action dated March 25, 2004, please consider the following remarks.

II. STATUS OF CLAIMS

Claims 1-23 are pending in the application.

Claims 1-23 were rejected under 35 U.S.C. §102(e) as being anticipated by Rallis, U.S. Patent No. 6,216,230 (hereinafter Rallis, or the Rallis reference).

III. STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the final Office Action.

IV. ISSUES PRESENTED FOR REVIEW

Whether claims 1-23 are patentable under 35 U.S.C. § 102(e) over U.S. Patent No. 6,216,230, issued to Rallis (hereinafter, the Rallis reference).

V. GROUPING OF CLAIMS

The rejected claims do not stand or fall together. Each claim is independently patentable. Separate arguments for the patentability of each claim are provided below.

VI. ARGUMENTS

A. The Independent Claims Are Patentable Over The Prior Art

1. The Rallis Reference

U.S. Patent No. 6,216,230, issued April 10, 2001 to Rallis et al. discloses a notebook security system (NBS) that prevents unauthorized use of a computer. A program resident on the computer and implements a user-validation procedure. A key device carries a first serial number and an encryption key. A second serial number is stored in said computer, the second serial number being the serial number of a device internal to the computer. A mass storage device installed in said computer stor s a validation record. The validation record comprises an unencrypted portion and an encrypted portion, the unencrypted portion including a copy of said first serial number and said encrypted portion including a copy of said second serial number and a user personal identification number. The key device is interfaced to the computer. The first serial number and the encryption key are read from said key device in order to gain authorized use of said computer. The key device may be removed from the computer after authorized use of the computer has been gained, and during operation of the computer.

2. Differences Between the Rallis Reference and the Applicants' Invention

The Rallis reference does not disclose a system for securing a token from unauthorized use. Instead, Rallis teaches the use of a token to prevent unauthorized use of a notebook computer. To achieve this aim, the Rallis reference discloses a system wherein the PIN is entered by a conventional keyboard coupled to a host computer, not by a device coupled between a token and the host computer, as described in the Applicants' invention. Rallis also does not disclose intercepting PIN commands from the host computer ... in fact, no message having a PIN is ever sent to the key. The only message sent to the key is a "super key" which is stored in the computer (BIOS), not something that the user entered.

The Final Office Action disagrees, stating:

> Although the Rallis reference does disclose preventing an unauthorized user to use a computer. Rallis also discloses that the key device (20) is used in conjunction with the computer to validate the user to perform operations (see col. 2, lines 45-67).

However, whether the Rallis reference discloses a key device "used in conjunction with a computer to validate the user to perform operations" is not the issue … the issue is whether Rallis teaches a system for preventing unauthorized use of a token. Simple examination of the Rallis reference reveals that it does not.

3. Independent Claim 1 is Patentable Over the Rallis Reference

Claim 1 recites:

> *receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol;*
>
> *accepting a PIN entered into the PIN entry device; and*
>
> *transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path.*

The First Office Action indicated that the Rallis reference disclosed the step of *"receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol"* as follows:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. (col. 1, lines 49-54)

The Applicants respectfully disagreed, pointing out that the foregoing teaches that the user connects the key to the notebook computer and enters a PIN into the notebook computer. Accordingly, there is no "PIN entry device" except perhaps the "notebook computer" which cannot be connected to itself via a USB protocol, as recited in claim 1.

In finally rejecting the Applicants' claims, the Examiner disagreed, arguing:

> "Rallis discloses this because a user is prompted to connect a key device (20) to the computer and the user transmits a pin to the notebook computer via the usb protocol."

Of course, even if the foregoing were true, this wordsmithed version of claim 1 does not address the issue at hand, that is, whether the foregoing discloses *"receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol."* Plainly, it does not.

In arguing that the Rallis reference discloses *"receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol"*, the Final Office Action relies on the foregoing passage (col. 1, lines 49-54), FIG. 1A (reproduced below), and the following text.

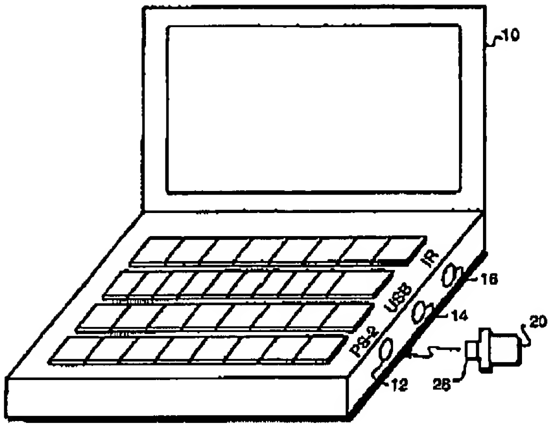

FIG. 1A

> FIG. 1A shows a key device 20 connected to a notebook computer 10. The key device 20, shown in FIG. 1B, has no external controls and is comprised of a microcomputer 22, a read-only-memory 24 and a connector 26. The connector 26 may attach to one of the I/O ports on the notebook computer 10. The preferred key device connection is via a PS-2 connector 12, although alternative connections, such as a Universal Serial Bus (USB) 14 and an Infra-Red (IR) port 16, can be used as described below. Although the security system has been designed for use with a notebook computer 10, it will be recognized that the system can be adapted for use with other computers, such as a desktops or Personal Digital Assistants (PDA). (col. 2, lines 35-47)

Clearly, nothing in FIG. 1A and in the above text discloses *"receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol"*, as recited in claim 1.

The First Office Action also indicated that the Rallis reference discloses the step of *"transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path"* as follows:

> The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. (col. 1, lines 54-59)

The Applicants responded by pointing out that the foregoing does not disclose transmitting a second message comprising a PN from a PIN entry device to a token. Rallis teaches a system wherein the PIN is entered into the notebook computer and used for further processing. It is not transmitted anywhere, let alone via from a PIN entry device to a token. In the Final Office Action, the Examiner disagreed, stating:

> "The Examiner disagrees that Pin is transmitted in second message, because Rallis discloses messages are transmitted to and from the key device (20) and the notebook computer (see col. 2, lines 48-60)"

Of course, the issue isn't whether messages are transmitted between the host computer and the key, but whether Rallis discloses *"transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path".* The passage relied upon is reproduced below:

> Ideally, the key device 20 is of such shape and size as to be placed on the user's key chain. It receives power and command messages from the notebook computer 10 and returns response messages, a serial number and an encryption key. A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. For maximum security protection, the key device 20 is connected only during the user-validation procedure and is carried and stored separately from the notebook computer 10. (col. 2, lines 48-60)

While the foregoing may disclose message transmission, it does not disclose *"transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path"*, as claim 1 requires.

Finally, Rallis discloses an embodiment in which the keyboard is separate from the host computer. That embodiment is shown below in a modified version of FIG. 5E:

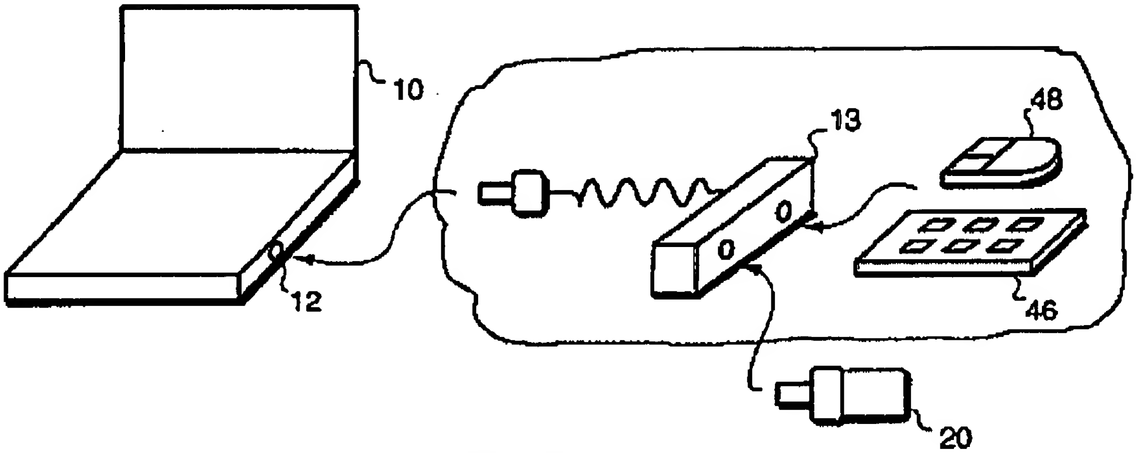

FIG. 5E

In another alternative a PS-2 "Y" connector 13, equipped with an internal automatic switch (not shown), is employed to permit the simultaneous PS-2 connection of a key device 20 and a keyboard 46 (or mouse 48) to a notebook computer 10 as shown in FIG. 5E. In a similar alternative, the key device 20 is connected to the keyboard port 18 of a desktop computer 11 via a AT "Y" connector 19, equipped with an internal automatic switch (not shown), that also permits the simultaneous connection of an AT keyboard 47 as shown in FIG. 5F. (col. 5, lines 12-22)

One might be tempted to argue that the circled items are the "PIN entry device" and that these elements together read on claim 1. However, even if the circled elements *receive a first message transmitted from a host processing device addressed to a pin entry device according to a universal serial bus (USB) protocol*, and *accept a PIN entered into the PIN entry device*, they do not *transmit a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path.* That is because the PIN is *not* transmitted to the token.

For the foregoing reasons, the rejection of claim 1 is respectfully traversed.

4. Claim 12 is Patentable Over the Rallis Reference

Claim 12 recites:

> *a PIN entry device, communicably coupleable to a host processing device transmitting a first message addressed to the PIN entry device, and communicatively coupleable to the token according to a universal serial bus USB protocol, the PIN entry device comprising:*
>
> *a user input device, for accepting a user-input PIN; and*

> *a processor, communicatively coupled to the user input device, the processor for receiving the first message and combining the first message with the user-input PIN, and for producing a second message having at least a portion of the first message and the user-input PIN*

Rallis does not disclose a PIN entry device having a processor that receives the message and combines it with a user-entered PIN to produce a second message. Accordingly, the rejection of claim 12 is traversed as well.

5. Claim 18 is Patentable Over the Rallis Reference

Claim 18 recites:

> *A method for securing a token from unauthorized use, comprising:*
> *intercepting a first message from the host processing device addressed to the token in a hub;*
> *providing the intercepted message to a PIN entry device communicatively coupled to the hub;*
> *accepting a second message from the PIN entry device comprising a user-entered PIN;*
> *generating a third message from the second message, the third message comprising the user-entered PIN and at least a portion of the first message; and*
> *transmitting the third message from the USB-compliant hub to the token.*

According to the First Office Action, the limitations of claim 18 were already discussed in the rejections of claims 1 and 3-4, but this is not the case. Nothing in Rallis discloses intercepting a message from a host processing device addressed to the token in a hub. Rallis, in fact, fails to disclose intercepting any message, fails to disclose sending a message from a host processing device to a token, and fails to disclose a hub at all. The First Office Action did not indicate which messages are the "second" and "third" messages described in the claim, and the Applicants can ascertain no such disclosure. Accordingly, the Applicants traversed the rejection of claim 18.

The Final Office Action offers no further insight, except to say that Rallis discloses transmitting messages that include the PIN, and the "hub" was addressed in other claims. The Applicants traverse this rejection.

6. Claim 20 is Patentable Over the Rallis Reference

Claim 20 recites:

> *a USB-compliant hub, communicably coupleable between a host processing device and the token, the USB compliant hub having;*
>
> *means for intercepting a message addressed to the PIN entry device;*
>
> *means for generating a third message from the first message and a user-entered PIN; and*
>
> *means for transmitting the third message to the token;*
>
> *a PIN entry device, communicatively coupled to USB-compliant hub, for accepting a user-entered PIN and providing the user-entered PIN to the USB-compliant hub.*

The First Office Action asserted that Rallis inherently discloses a USB-compliant hub, because it discloses a USB-compliant port.

The Applicants responded that a USB hub is not analogous to a USB port, and nothing in the Rallis reference indicates that a USB hub is necessarily present, as the law of "inherency" requires. *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1269(Fed. Cir. 1991). The Applicants also pointed out that Rallis fails to disclose a PIN entry device.

In finally rejecting claim 3, the Examiner again appears to argue that a USB port inherently discloses a USB hub. On this issue, the Examiner and the Applicants will continue to disagree … a USB port does not necessarily include a USB hub.

The Final Office Action also provides "proof" that indicates a "system that has a usb port is a usb hub", citing the following portion of U.S. Patent 6,038,320, issued to Miller:

> The computer 20, like the computer 10 in FIG. 1, includes a CPU 12, a BIOS flash memory 24 and a keyboard controller 18 coupled to a data/address bus 16. Further coupled to the data/address bus 16 is a USB controller 26. The USB controller 26 is also coupled to a USB port 31 through a USB 28. A USB hub 30 is plugged into the USB port 31 to allow more devices to be coupled to the USB 28 through USB port 31. The USB hub 30 includes multiple USB ports 32. A USB keyboard 34 is plugged into a USB port 32 of the USB hub 30. (col. 1, line 60 – col. 2, line 2)

Of course, the above passage, at best, discloses that a *hub* inherently includes a *port*, not that a *port* inherently includes a *hub*. It is simply untrue that a system with a USB port necessarily includes a USB hub.

The remaining features of claim 20 are likewise not disclosed by Rallis. Accordingly, the rejection of claim 20 is traversed.

B. The Dependent Claims Are Patentable Over The Prior Art

1. Dependent Claim 2 is Patentable Over the Rallis Reference

Claim 2 recites that the first message received in the PIN entry device and the second message is transmitted from the PIN entry device directly to the token along the secure communication path. The First Office Action rejected claim 2, based on the following portions of the Rallis reference:

> The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. (col. 1, lines 51-54)

and at

> The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 1, lines 60-67)

and

> A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. For maximum security protection, the key device 20 is connected only during the user-validation procedure and is carried and stored separately from the notebook computer 10. (col. 2, lines 52-56)

Plainly, the Rallis reference does not teach transmitting a PIN to the token at all, let alone via a USB protocol. Accordingly, the Applicants traversed the rejection of claim 2.

The Final Office Action rejected claim 2 on the same basis as claim 1, and thus provides no further insight regarding the rejection. Accordingly, the Applicants respectfully traverse this rejection.

2. Dependent Claim 3 is Patentable Over the Rallis Reference

Claim 3 recites that the step of receiving the first message from the host processing device and addressed to a PIN entry device comprises the steps of:

> *receiving the first message in a USB-compliant hub communicatively coupled to the host processing device via a first communication path; and*
>
> *transmitting the first message to the PIN entry device communicatively coupled to the USB-compliant hub*

and that the step of transmitting the second message comprising a portion of the first message and the PIN and at least a portion of the first message from the PIN entry device to the token along a secure communication path comprises the step of:

> *transmitting a second message from the PIN entry device via the USB hub.*

As described above with respect to claim 20, Rallis does not disclose a USB hub. The remaining features of claim 3, in terms of messages having particular information, transmitted from one entity to another, are also not disclosed by Rallis. Accordingly, the rejection of claim 3 is improper and should be reversed.

3. Dependent Claim 4 is Patentable Over the Rallis Reference

Claim 4 recites that the step of transmitting the second message from the PIN entry device via the USB-compliant hub comprises the steps of:

> *transmitting a third message comprising the PIN from the PIN entry device to the USB-compliant hub;*
>
> *processing the message in the USB-compliant hub to produce the second message; and*
>
> *transmitting the second message from the USB-compliant hub.*

According to the First Office Action, the foregoing steps are disclosed as follows:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 1, lines 49-67).

The Applicants traversed, as nothing in the foregoing text discloses transmitting a third message comprising the PIN from the PIN entry device to a USB-compliant hub, processing the message in the hub to produce a second message, or transmitting the second message from the USB-compliant hub. Rallis fails to discloses a hub and teaches that the PIN is accepted in the notebook computer and is not transmitted anywhere else.

The Final Office Action provided no further rationale for the rejection of claim 4.

4. Dependent Claim 5 is Patentable Over the Rallis Reference

Claim 5 recites the features of claim 1, and is patentable on the same basis.

5. Dependent Claims 6, 7, 8, 9, 13, 15, and 22-23 are Patentable Over the Rallis Reference

Claim 6 recites that the first message (transmitted from a host processing device and addressed to a PIN entry device according to a USB protocol) is encrypted according to a first encryption key, and that the entry device comprises a decryption module having access to the first encryption key for decoding the first message. The First Office Action indicates that this was disclosed as follows:

> Briefly, a security system constructed in accordance with the invention implements a user-validation procedure that requires the user to connect the proper hardware "key" device to a computer at power-up to enable operation. The system can support multiple users and a single supervisor. Each authorized user is provided with a unique key device which is carried and stored separately from the computer. The key device holds a unique serial number and an encryption key. A validation record stored on the computer's hard disk contains an unencrypted key device serial number, an encrypted hard disk serial number, and a Personal Identification Number (PIN) unique to the user.
>
> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 1, lines 37-67)

The Applicants pointed out that the foregoing does not teach a PIN entry device having a decryption module for decoding the first message.

The Final Office Action answered:

> "Rallis discloses that there is a matching decrypted pin, thus the pin that is entered is encrypted. Further Rallis also discloses an encryption key that has a corresponding decryption key (see col. 1, lines 49-64)"

The cited portion of the Rallis reference is reproduced below:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device.

The foregoing exerpt discloses the storage of an encrypted PIN in the laptop computer that is decrypted (by a program automatically invoked by the host computer at power-up) and compared to a PIN that is manually entered into the laptop computer. While this discloses a PIN and a decrypted PIN, it does not disclose the features of claim 6, namely, the encryption of a first message transmitted from a host processing device and addressed to a PIN entry device.

Claim 13 is allowable for the same reasons. Claims 8 and 15 likewise recite decryption modules that are not needed or employed in Rallis. Accordingly, the Applicants respectfully traverse the rejection of claims 6, 8, 9, 13, and 15.

6. Dependent Claims 10-11 are Patentable Over the Rallis Reference

Claims 10 and 11 recite the features of claim 1, and are patentable on the same basis.

7. Dependent Claims 14, 16, 17, 19, and 21 are Patentable Over the Rallis Reference

Claims 14, 16, and 17, and claims 19 and 21 recite the features of claims 12 and 18, respectively, and are patentable on the same basis.

VII. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: **May 25, 2004**

By: ______________________
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/amb

G&C 30074.29-US-I1